

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-231760

(P2000-231760A)

(43) 公開日 平成12年8月22日 (2000.8.22)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	データベース <sup>*</sup> (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D
G 1 1 B 19/04	5 0 1	G 1 1 B 19/04	5 0 1 H
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A

審査請求 未請求 請求項の数23 O L (全 12 頁)

(21) 出願番号 特願平11-344396

(22) 出願日 平成11年12月3日 (1999.12.3)

(31) 優先権主張番号 特願平10-352975

(32) 優先日 平成10年12月11日 (1998.12.11)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番5号

(72) 発明者 浅野 智之

東京都品川区北品川6丁目7番5号 ソニ

ー株式会社内

(72) 発明者 大澤 義知

東京都品川区北品川6丁目7番5号 ソニ

ー株式会社内

(74) 代理人 100082131

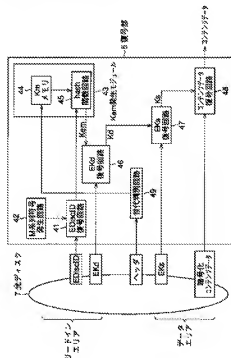
弁理士 稲本 義雄

(54) 【発明の名称】 情報記録装置および方法、情報再生装置および方法、並びに記録媒体

## (57) 【要約】

【課題】 秘密キーを更新した場合でも、古い世代の秘密キーを用いて暗号化データを復号できるようにする。

【解決手段】 光ディスク7には、暗号化コンテンツデータを暗号化したセクタキー-Eksの世代が書き込まれている。世代判別回路49は、暗号化に用いられたセクタキー-Eksの世代を判別する。Kmメモリ44は、判別された世代に対応したマスタキー-KmをEkd復号回路46に出力する。Ekd復号回路46は、暗号化されたディスクキー-Ekdを、マスタキー-Kmを用いて復号する。Ekd復号回路47は、ディスクキー-Kdを用いて、暗号化されたセクタキー-Eksを復号し、セクタキー-Ksを得る。コンテンツデータ復号回路48はセクタキー-Ksを用いて、暗号化コンテンツデータを復号する。



**【特許請求の範囲】**

【請求項1】 着脱可能な記録媒体にデータを記録する情報記録装置において、少なくとも1以上の世代の秘密鍵を記憶する記憶手段と、

前記記録媒体の媒体識別情報と前記秘密鍵から第1の鍵を生成する生成手段と、  
前記記録媒体に記録する前記データを暗号化するために用いる第2の鍵を前記第1の鍵で暗号化する第1の暗号化手段と、

前記第1の暗号化手段により暗号化された前記第2の鍵を、前記第1の鍵の世代番号とともに前記記録媒体に記録する第1の記録手段とを備えることを特徴とする情報記録装置。

【請求項2】 前記媒体識別情報を、乱数として発生させる第1の乱数発生手段をさらに備え、  
前記第1の暗号化手段は、前記記録媒体が予め前記第2の鍵を有している場合、前記記録媒体から前記第2の鍵を読み出し、前記記録媒体が前記第2の鍵を有していない場合、前記第1の乱数発生手段に前記第2の鍵となる乱数を発生させることを特徴とする請求項1に記載の情報記録装置。

【請求項3】 前記記録媒体は、複数の記録単位に分割されており、  
前記記録単位に記録する前記データを暗号化する第3の鍵となる乱数を前記記録単位毎に発生させる第2の乱数発生手段と、  
前記第2の乱数発生手段により発生された前記第3の鍵を、前記第2の鍵で暗号化する第2の暗号化手段と、  
前記第2の暗号化手段により暗号化された前記第3の鍵を前記記録媒体の記録単位に記録する第2の記録手段とをさらに備えることを特徴とする請求項2に記載の情報記録装置。

【請求項4】 前記第2の鍵は、前記記録媒体毎に固有の値とされるときに、前記秘密鍵の世代が変わる毎に、前記第1の乱数発生手段により新規に生成されることを特徴とする請求項2に記載の情報記録装置。

【請求項5】 前記記憶手段は、1世代の前記秘密鍵を記憶し、演算により他の世代の前記秘密鍵を生成することを特徴とする請求項1に記載の情報記録装置。

【請求項6】 前記第1の鍵の世代番号は、前記生成手段で用いた前記秘密鍵の世代に対応することを特徴とする請求項1に記載の情報記録装置。

【請求項7】 着脱可能な記録媒体にデータを記録する情報記録装置の情報記録方法において、少なくとも1以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、  
前記記録媒体の媒体識別情報と前記秘密鍵から第1の鍵を生成する生成ステップと、  
前記記録媒体に記録するデータを暗号化するために用い

る第2の鍵を前記第1の鍵で暗号化する第1の暗号化ステップと、

前記第1の暗号化ステップの処理により暗号化された前記第2の鍵を、前記第1の鍵の世代番号とともに前記記録媒体に記録するように記録を制御する第1の記録制御ステップを含むことを特徴とする情報記録方法。

【請求項8】 前記媒体識別情報を、乱数として発生させる第1の乱数発生ステップをさらに含み、

前記第1の暗号化ステップの処理では、前記記録媒体が予め前記第2の鍵を有している場合、前記記録媒体から前記第2の鍵を読み出し、前記記録媒体が前記第2の鍵を有していない場合、前記第1の乱数発生ステップの処理により前記第2の鍵となる乱数を発生させることを特徴とする請求項7に記載の情報記録方法。

【請求項9】 前記記録媒体は、複数の記録単位に分割されており、  
前記記録単位に記録する前記データを暗号化する第3の鍵となる乱数を前記記録単位毎に発生させる第2の乱数発生ステップと、  
前記第2の乱数発生ステップの処理により発生された前記第3の鍵を、前記第2の鍵で暗号化する第2の暗号化ステップと、

前記第2の暗号化ステップの処理により暗号化された前記第3の鍵を前記記録媒体の記録単位に記録するように記録を制御する第2の記録制御ステップとをさらに含むことを特徴とする請求項8に記載の情報記録方法。

【請求項10】 前記第2の鍵は、前記記録媒体毎に固有の値とされるときに、前記秘密鍵の世代が変わる毎に、前記第1の乱数発生ステップの処理により新規に生成されることを特徴とする請求項8に記載の情報記録方法。

【請求項11】 前記記憶制御ステップの処理では、1世代の前記秘密鍵を記憶するように記憶を制御し、演算により他の世代の前記秘密鍵を生成することを特徴とする請求項7に記載の情報記録方法。

【請求項12】 前記第1の鍵の世代番号は、前記生成ステップの処理で用いた前記秘密鍵の世代に対応することを特徴とする請求項7に記載の情報記録方法。

【請求項13】 着脱可能な記録媒体にデータを記録する情報記録装置用のプログラムであって、  
少なくとも1以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、  
前記記録媒体の媒体識別情報と前記秘密鍵から第1の鍵を生成する生成ステップと、  
前記記録媒体に記録するデータを暗号化するために用いる第2の鍵を前記第1の鍵で暗号化する暗号化ステップと、  
前記暗号化ステップの処理により暗号化された前記第2の鍵を、前記第1の鍵の世代番号とともに前記記録媒体に記録するように記録を制御する記録制御ステップとを

含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項14】 着脱可能な記録媒体に記録されているデータを再生する情報再生装置において、少なくとも1以上の世代の秘密鍵を記憶する記憶手段と、

前記記録媒体から、第1の鍵で暗号化された第2の鍵、前記第2の鍵を暗号化した前記第1の鍵の世代番号、および前記記録媒体の媒体識別情報を読み出す第1の読み出し手段と、

前記第1の読み出し手段により読み出された前記媒体識別情報および前記世代番号に対応する前記秘密鍵から前記第1の鍵を生成する生成手段と、

前記生成手段により生成された前記第1の鍵で、前記第2の鍵を復号する第1の復号手段とを備えることを特徴とする情報再生装置。

【請求項15】 前記記録媒体は、複数の記録単位に分割されており、

前記記録単位に記録されている前記第2の鍵で暗号化された第3の鍵を読み出す第2の読み出し手段と、

前記第1の復号手段により復号された前記第2の鍵で、前記第2の読み出し手段により読み出された前記第3の鍵を復号する第2の復号手段と、

前記第2の復号手段により復号された前記第3の鍵で、前記データを復号する第3の復号手段とをさらに備えることを特徴とする請求項14に記載の情報再生装置。

【請求項16】 前記記憶手段は、1世代の前記秘密鍵を記憶し、演算により他の世代の前記秘密鍵を生成することを特徴とする請求項14に記載の情報再生装置。

【請求項17】 前記第1の鍵の世代番号は、前記生成手段で用いた前記秘密鍵の世代に対応することを特徴とする請求項14に記載の情報再生装置。

【請求項18】 着脱可能な記録媒体に記録されているデータを再生する情報再生装置の情報再生方法において、

少なくとも1以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、

前記記録媒体から、第1の鍵で暗号化された第2の鍵、前記第2の鍵を暗号化した前記第1の鍵の世代番号、および前記記録媒体の媒体識別情報を読み出す第1の読み出しステップと、

前記第1の読み出しステップの処理により読み出された前記媒体識別情報および前記世代番号に対応する前記秘密鍵から前記第1の鍵を生成する生成ステップと、

前記生成ステップの処理により生成された前記第1の鍵で、前記第2の鍵を復号する第1の復号ステップとを含むことを特徴とする情報再生方法。

【請求項19】 前記記録媒体は、複数の記録単位に分割されており、前記記録単位に記録されている前記第2の鍵で暗号化さ

れた第3の鍵を読み出す第2の読み出しステップと、前記第1の復号ステップの処理により復号された前記第2の鍵で、前記第2の読み出しステップの処理により読み出された前記第3の鍵を復号する第2の復号ステップと、

前記第2の復号ステップの処理により復号された前記第3の鍵で、前記データを復号する第3の復号ステップとをさらに含むことを特徴とする請求項18に記載の情報再生方法。

【請求項20】 前記記憶制御ステップの処理では、1世代の前記秘密鍵を記憶し、演算により他の世代の前記秘密鍵を生成することを特徴とする請求項18に記載の情報再生方法。

【請求項21】 前記第1の鍵の世代番号は、前記生成ステップの処理で用いた前記秘密鍵の世代に対応することを特徴とする請求項18に記載の情報再生方法。

【請求項22】 着脱可能な記録媒体に記録されているデータを再生する情報再生装置用のプログラムであって、

少なくとも1以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、

前記記録媒体から、第1の鍵で暗号化された第2の鍵、前記第2の鍵を暗号化した前記第1の鍵の世代番号、および前記記録媒体の媒体識別情報を読み出す読み出しステップと、

前記読み出しステップの処理により読み出された前記媒体識別情報および前記世代番号に対応する前記秘密鍵から前記第1の鍵を生成する生成ステップと、

前記生成ステップの処理により生成された前記第1の鍵で、前記第2の鍵を復号する復号ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項23】 情報記録装置または情報再生装置によりデータが記録または再生される記録媒体において、前記記録媒体に固有の値である媒体識別情報と、

前記媒体識別情報と前記情報記録装置からの秘密鍵により生成される第1の鍵で暗号化された、前記データを暗号化するために用いる前記第2の鍵とが記録されているとともに、

前記第1の鍵で暗号化されている前記第2の鍵は、前記第1の鍵の世代番号と関連付けられて記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報記録装置および方法、情報再生装置および方法、並びに記録媒体に関し、特に、著作権を有するコンテンツが不正に利用されることなく、安全に暗号化されたコンテンツを記録媒体に記録または再生できるようにした情報記録装置および方法、情報再生装置および方法、並びに記録媒体に関する

る。

【0002】

【従来の技術】近年、情報をデジタル的に記録する記録機器および記録媒体が普及しつつある。これらの記録機器および記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽の著作権者にしてみれば、自らが著作権を有する映像や音楽のデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録機器および記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ要路がある。

【0003】例えば、ミニディスク（MD）（商標）システムにおいては、SCMS(Serial CopyManagement System)と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報により、音楽データが、copy free（コピー自由）、copy once allowed（コピー1回可）、またはcopy prohibited（コピー禁止）のうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。

【0004】このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正にコピーされるのが防止されている。

【0005】また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk(DVD)（商標）システムにおける、コンテンツスクランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録機器だけが暗号鍵を与えられ、これにより暗号化されているデータを復号し、意味のあるデータを得ることができるようにされている。そして、記録機器は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされることが防止されている。

【0006】しかしながら、ミニディスクシステムが採用している方式では、SCMSがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録されるなどの動作規定に従わない記録機器が、不正に製造されると、それによるコピーを防止することができない。

【0007】また、DVDシステムが採用している方式は、ROM(Read Only Memory)メディアに対しては有効

であるが、ユーザがデータを記録可能なRAM(Random Access Memory)メディアにおいては有効ではない。RAMメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録機器で動作するディスクを新たに作ることができるからである。

【0008】そこで、本出願人は、先に提出した特願平10-25310において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、ライセンスを受けた機器でしか、その記録媒体の媒体識別情報にアクセスできないようにする方法を提案した。その方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない機器がその暗号化されたデータを読み出したとしても、そのデータは意味をなさないようにしている。各機器はライセンスを受ける際、不正な複製ができないようにその動作が規定されている。

【0009】ライセンスを受けていない機器は媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない機器がアクセス可能な全ての情報（暗号化されている）を新たな媒体に複製したとしても、そのようにして作成された媒体の情報は、ライセンスを受けていない機器は勿論、ライセンスを受けた機器においても、正しく読み出す事ができない。このようにして、不正な複製が行われる事が防止されている。

【0010】

【発明が解決しようとする課題】先の提案におけるライセンスにより得られる秘密キーは、全機器において共通である必要があった。これは、1つの機器で記録された媒体が、他の機器で再生可能である（インターオペラビリティを確保する）為に必要な条件であった。

【0011】この為に、1つの機器が攻撃者により攻撃を受け、その機器が保持していた秘密キーが暴かれたしまった場合、全ての機器の秘密キーが暴かれてしまったのと同じ事になり、すなわち、秘密キーが暴かれる前に記録されたデータは勿論、秘密キーが暴かれた後に記録されたデータも、その暴かれた秘密キーを用いて、解読してしまうといった課題があった。

【0012】そのようなことを防ぐために、秘密キーが暴かれたことがわかったときや、定期的に、機器に記憶されている秘密キーを更新することが考えられる。更新された秘密キーが用いられることにより、その秘密キーで暗号化されたデータは、暴かれた秘密キーでは解読されないことになる。

【0013】しかしながら、上述したように、機器に記憶されている秘密キーを更新した場合、古い秘密キーを

用いて暗号化されたデータが復号できなくなるといった課題があった。

【0014】本発明はこのような状況に鑑みてなされたものであり、秘密キーを古い世代のキーも含めて複数記憶するか、または、最新世代の秘密キーから古い世代の秘密キーを作成できるようにすることにより、機器に記憶されている秘密キーを更新した場合でも、古い世代の秘密キーを利用して暗号化されたデータを復号できるようにするものである。

【0015】

【課題を解決するための手段】請求項1に記載の情報記録装置は、少なくとも1以上の世代の秘密鍵を記憶する記憶手段と、記録媒体の媒体識別情報と秘密鍵から第1の鍵を生成する生成手段と、記録媒体に記録するデータを暗号化するために用いる第2の鍵を第1の鍵で暗号化する第1の暗号化手段と、第1の暗号化手段により暗号化された第2の鍵を、第1の鍵の世代番号とともに記録媒体に記録する第1の記録手段とを備えることを特徴とする。

【0016】請求項7に記載の情報記録方法は、少なくとも1以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、記録媒体の媒体識別情報と秘密鍵から第1の鍵を生成する生成ステップと、記録媒体に記録するデータを暗号化するために用いる第2の鍵を第1の鍵で暗号化する第1の暗号化ステップと、第1の暗号化ステップの処理により暗号化された第2の鍵を、第1の鍵の世代番号とともに記録媒体に記録するように記録を制御する第1の記録制御ステップとを含むことを特徴とする。

【0017】請求項13に記載の記録媒体のプログラムは、少なくとも1以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、記録媒体の媒体識別情報と秘密鍵から第1の鍵を生成する生成ステップと、記録媒体に記録するデータを暗号化するために用いる第2の鍵を第1の鍵で暗号化する第1の暗号化ステップと、暗号化ステップの処理により暗号化された第2の鍵を、第1の鍵の世代番号とともに記録媒体に記録するように記録を制御する記録制御ステップとを含むことを特徴とする。

【0018】請求項14に記載の情報再生装置は、少なくとも1以上の世代の秘密鍵を記憶する記憶手段と、記録媒体から、第1の鍵で暗号化された第2の鍵、第2の鍵を暗号化した第1の鍵の世代番号、および記録媒体の媒体識別情報を読み出す第1の読み出し手段と、第1の読み出し手段により読み出された媒体識別情報および世代番号に対応する秘密鍵から第1の鍵を生成する生成手段と、生成手段により生成された第1の鍵で、第2の鍵を復号する第1の復号手段とを備えることを特徴とする。

【0019】請求項18に記載の情報再生方法は、少な

くとも1以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、記録媒体から、第1の鍵で暗号化された第2の鍵、第2の鍵を暗号化した第1の鍵の世代番号、および記録媒体の媒体識別情報を読み出す第1の読み出しステップと、第1の読み出しステップの処理により読み出された媒体識別情報および世代番号に対応する秘密鍵から第1の鍵を生成する生成ステップと、生成ステップの処理により生成された第1の鍵で、第2の鍵を復号する第1の復号ステップとを含むことを特徴とする。

【0020】請求項22に記載の記録媒体のプログラムは、少なくとも1以上の世代の秘密鍵を記憶するように記憶を制御する記憶制御ステップと、記録媒体から、第1の鍵で暗号化された第2の鍵、第2の鍵を暗号化した第1の鍵の世代番号、および記録媒体の媒体識別情報を読み出す読み出しステップと、読み出しステップの処理により読み出された媒体識別情報および世代番号に対応する秘密鍵から第1の鍵を生成する生成ステップと、生成ステップの処理により生成された第1の鍵で、第2の鍵を復号する復号ステップとを含むことを特徴とする。

【0021】請求項23に記載の記録媒体は、記録媒体に固有の値である媒体識別情報と、媒体識別情報と情報記録装置からの秘密鍵により生成される第1の鍵で暗号化された、データを暗号化するために用いる第2の鍵とが記録されているとともに、第1の鍵で暗号化されている第2の鍵は、第1の鍵の世代番号と関連付けられて記録されていることを特徴とする。

【0022】請求項1に記載の情報記録装置、請求項7に記載の情報記録方法、および請求項13に記載の記録媒体のプログラムにおいては、少なくとも1以上の世代の秘密鍵が記憶され、記録媒体の媒体識別情報と秘密鍵から第1の鍵が生成され、記録媒体に記録するデータを暗号化するために用いる第2の鍵が第1の鍵で暗号化され、暗号化された第2の鍵が第1の鍵の世代番号とともに記録媒体に記録される。

【0023】請求項14に記載の情報再生装置、請求項18に記載の情報再生方法、および請求項22に記載の記録媒体のプログラムにおいては、少なくとも1以上の世代の秘密鍵が記憶され、記録媒体から、第1の鍵で暗号化された第2の鍵、第2の鍵を暗号化した第1の鍵の世代番号、および記録媒体の媒体識別情報を読み出され、読み出された媒体識別情報および世代番号に対応する秘密鍵から第1の鍵が生成され、生成された第1の鍵で、第2の鍵が復号される。

【0024】請求項23に記載の記録媒体においては、記録媒体に固有の値である媒体識別情報と、媒体識別情報と情報記録装置からの秘密鍵により生成される第1の鍵で暗号化された、データを暗号化するために用いる第2の鍵とが記録されているとともに、第1の鍵で暗号化されている第2の鍵は、第1の鍵の世代番号と関連付け

られて記録されている。

【0025】

【発明の実施の形態】以下に本発明の実施の形態を説明する。図1は、本発明を適用した光ディスク記録再生装置の構成例を表している。入力部1は、ボタン、スイッチ、リモートコントロールなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。例えば、マイクロコンピュータなどにより構成される制御回路2は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。

【0026】記録再生回路3は、暗号化部4と復号部5を有し、復号部5は、ピックアップ6により、光ディスク7から再生されたデータを復号し、再生信号として外部に出力する。暗号化部4は、外部から記録信号の供給を受け取ると、これを暗号化し、ピックアップ6に供給して、光ディスク7に記録させる。

【0027】ピックアップ6は、レーザビームを光ディスク7に照射することで、データの記録再生を行う。スピンドルモータ9は、サーボ回路8によって制御され、光ディスク7を回転させる。サーボ回路8は、スピンドルモータ9を駆動することにより、光ディスク7を所定の速度で（例えば線速度一定で）回転させる。サーボ回路8はまた、ピックアップ6のトラッキングおよびフォーカシングの他、スレッドサーボを制御する。乱数発生回路10は、制御回路2の制御により、所定の乱数を発生する。

【0028】光ディスク7には、図2に示すような構造を有するデータが記録されている。光ディスク7のリードインエリアには、光ディスク7のID（以下、DiscIDと称する）を、予め定められたM系列符号で暗号化したDiscID、世代番号と関連づけられたディスクキー-Kdをイフエクティブマスター-Keyemで暗号化した暗号化ディス

イフエクティブマスター-Keyem=hash（マスター-Keym+DiscID）・・・（1）

ここでマスター-Keymは、著作権者等から適正にライセンスを受けた者（光ディスク記録再生装置）にだけ与えられる秘密のキーである。また、ここで、例えば、AとBの結合とは、それぞれが32ビットであるとき、Aの後ろにBを結合して、64ビットのデータとすることを意味する。

【0033】光ディスク7のデータエリアの各セクタSi（i=1,2,...）は、ヘッダおよびメインデータ部で構成され、ヘッダには、セクタキー-Ksiをディスクキー-Kdで暗号化した暗号化セクタキー-Eksi（i=1,2,...）が格納されている（ここでKsiのiは、セクタの番号を示し、セクタキーはセクタ毎に異なるのでKsiと記述するが、特に区別する必要がない場合は、Ksとも記述する）。

【0034】また、光ディスク7には、複数の世代のディスクキー-Kd（イフエクティブマスター-Keyemにより暗号化されている）が記録されているので、どの世代のディスクキーが用いられて暗号化されたのかを識別できる

クキー-Ekdが記録されている。図2に示した例では、世代番号1と世代番号3の暗号化ディスクキー-Ekdが記録されている。

【0029】DiscIDとは、光ディスク7を識別するための異なる固有の値である。また、ディスクキー-Kdは、光ディスク7毎に固有の値であるとともに、記録再生回路3のマスタキー-Kmの世代番号毎にも異なる固有の値である。すなわち、マスタキー-Kmの世代が更新される毎に、それぞれの世代に対応するディスクキー-Kdj（j=1,2,3...）が存在する（ここでKdjのjは、世代番号を示すが、特に区別する必要がない場合は、Kdとも記述する）。

【0030】M系列符号は、所定の周期で、“0”と“1”の2値がランダムに出現する疑似ランダム2値信号（一種の疑似乱数）であり、DiscIDは、例えば、ファイル名やディレクトリ情報などのTOC（Table Of Contents）データ内に、予め設定された所定のM系列符号に基づいて埋め込むことで暗号化されている。すなわち、DiscIDは、TOCデータのエッジの時間ずれとして記録される。このような暗号化を行うと、TOCデータはM系列符号がなくとも読み取ることができる（TOCデータは暗号化されないが）、DiscIDはM系列符号がらりと読み取る（復号する）ことができなくなる。このようなM系列符号に基づく暗号化に関する技術は、特開平09-288960号として本出願人が先に提案している。なお、この所定のM系列符号は、著作権者から適正なライセンスを受ける際、後述するマスタキー-Kmとともに、ライセンスを受けた者に与えられる。

【0031】イフエクティブマスター-Keyemは、以下に示す式（1）に従い、マスタキー-KmとDiscIDの結合にhash関数を適用して計算される。

【0032】

（マスター-Keym+DiscID）・・・（1）

ように、データエリアの各セクタのヘッダには、用いられたディスクキー-Kdの世代番号も記録されている。図2に示した例では、光ディスク7に記録されているディスクキー-Kdの世代は、世代番号1と世代番号3であるので、その世代番号1と世代番号3のディスクキー-Kdのみが用いられてセクタキー-Eksiは暗号化されている。

【0035】メインデータ部には、コンテンツデータをセクタキー-Ksiで暗号化した暗号化コンテンツデータが格納されている。

【0036】図3は、暗号化部4の構成例を表している。DiscID暗号化復号回路21は、光ディスク7から読み出された暗号化ディスクID、すなわちDiscID、M系列符号発生回路22から供給されるM系列符号に基づいて復号し、DiscIDを生成する。DiscID暗号化復号回路21はまた、乱数発生回路10から発生された乱数をDiscIDとして受け取り、M系列符号発生回路22から供給されるM系列符号に基づいて、上述したように、入力さ

れるTOC情報に埋め込むように暗号化して、EdiscIDを生成し、光ディスク7に記録する。

【0037】M系列符号発生回路22は、例えば、直列接続された複数のフリップフロップとExclusive-OR（イクスクルーシブオア）回路から構成したり、あるいは、ROM、EEPROMなどで構成することもできる。

【0038】Ken発生モジュール23のKmメモリ24は、複数のマスターキーKmを記憶する。Ken発生モジュール23のhash関数回路25は、マスターキーKmとDiscIDの結合を生成し、これにChash関数を適用してイフェクティブマスターキーKenを算出する。

【0039】Kd暗号化復号回路26は、光ディスク7から読み出された暗号化ディスクキーEKdを、イフェクティブマスターキーKenで復号して、ディスクキーKdを生成する。Kd暗号化復号回路26はまた、乱数発生回路10から発生された乱数をディスクキーKdとして受け取り、イフェクティブマスターキーKenで暗号化して暗号化ディスクキーEKdを生成し、光ディスク7に記録する。

【0040】Ks暗号化回路27は、乱数発生回路10から発生された乱数をセクタキーKsとして受け取り、ディスクキーKdで暗号化して暗号化セクタキーEKsを生成し、光ディスク7に記録する。コンテンツデータ暗号化回路28は、セクタキーKsで、コンテンツデータを暗号化し、光ディスク7に記録する。

【0041】なお、図3の例では、暗号化回路として、Ks暗号化回路27とコンテンツデータ暗号化回路28を、それぞれ別々の構成として記載したが、これらは、勿論、一つの暗号化回路として構成してもよい（復号回路も同様である）。

【0042】次に、図4に、復号部5の構成例を示す。EdiscID復号回路41は、光ディスク7から読み出されたEdiscIDを、M系列符号発生回路42から供給されるM系列符号に基づいて復号して、DiscIDを生成する。M系列符号発生回路42は、M系列符号発生回路22と同様の構成を有し、M系列符号発生回路22と同一のM系列符号を発生するようになされている。

【0043】Ken発生モジュール43のKmメモリ44は、複数のマスターキーKmを記憶する。Ken発生モジュール43のhash関数回路45は、マスターキーKmとDiscIDの結合を生成し、これにChash関数を適用してイフェクティブマスターキーKenを計算する。このKen発生モジュール43は、Ken発生モジュール23と同一の構成とされ、両者を兼用するようにしてもよい。ここで、Kmメモリ24とKmメモリ44に記憶されるマスターキーについて、図5を参照して説明する。

【0044】Kmメモリ24、44には、マスターキーKmが、世代が若い順に複数記憶される。図5は、世代番号1乃至3のマスターキーKmが記憶されている例を示している。新たな世代のマスターキーKmは、例えば、その新たな世代のマスターキーKmが記録された光ディスク7を介して

配布されたり、インターネットなどのネットワークを介して配布される。マスターキーKmを記憶する各デバイス（光ディスク記録再生装置）毎に、そのデバイス固有の暗号鍵を保持させ、Kmメモリ24、44に記憶されるマスターキーKmを、その暗号鍵で暗号化してから記憶させるようにしても良い。

【0045】EKd復号回路46は、光ディスク7から読み出された暗号化ディスクキーEKdを、イフェクティブマスターキーKenで復号して、ディスクキーKdを算出する。EKs復号回路47は、光ディスク7から各セクタSiのヘッダに記録されている暗号化セクタキーEKsを読み出し、ディスクキーKdで復号して、セクタキーKsを算出する。コンテンツデータ復号回路48は、光ディスク7から読み出された暗号化されているコンテンツデータを、セクタキーKsで復号する。

【0046】世代判別回路49は、データエリアのヘッダを読み出し、メインデータ部に記録されているコンテンツデータが、どの世代のセクタキーKsを用いて暗号化されているかを判断し、その判断結果をKmメモリ44に出力する。Kmメモリ44は、世代判別回路49から出力された世代に関するデータに従って、記憶されているマスターキーKmをhash関数回路45に出力する。

【0047】次に、コンテンツデータが光ディスク7に記録される場合の暗号化部4における処理手順を、図6のフローチャートを参照して説明する。ステップS1において、DiscID暗号化復号回路21は、光ディスク7のリードインエリアに、EdiscIDが書き込まれているか否かの判定を行い、Kd暗号化復号回路26は、光ディスク7のリードインエリアに、暗号化ディスクキーEKdが書き込まれているか否かの判定を行う。EdiscIDと暗号化ディスクキーEKdが共に書き込まれていないと判定された場合、ステップS2に進み、乱数発生回路10は、128ビットの乱数を発生し、DiscIDとして、DiscID暗号化復号回路21に出力する。

【0048】ステップS3において、DiscID暗号化復号回路21は、乱数発生回路10から供給されたDiscIDを、M系列符号発生回路22から供給されたM系列符号に基づいて、上述したように、TOC情報中に埋め込むようにして暗号化して、EdiscIDを生成し、光ディスク7のリードインエリアに記録する。M系列符号回路22が供給するM系列符号は、著作権者から適正なライセンスを受けるときに与えられたものである。

【0049】次に、ステップS4において、Ken発生モジュール23のhash関数回路25は、Ken発生モジュール23のKmメモリ24から、最新世代のマスターキーKmを読み出す。Ken発生モジュール23のhash関数回路25は、ステップS5で、上述した式（1）に従い、光ディスク7のDiscID、およびKmメモリ24から読み出されたマスターキーKmの結合にhash関数を適用して、イフェクティブマスターキーKenを計算し、Kd暗号化復号回路26に供

給する。

【0050】次に、ステップS6において、乱数発生回路10は、40ビットの乱数を生じ、ディスクキーKdとして、Kd暗号化復号回路26に出力する。Kd暗号化復号回路26は、ステップS7において、乱数発生回路10から供給されたディスクキーKdを、hash関数回路25から受け取ったイフェクティブマスタキーKemにより暗号化して、暗号化ディスクキーEKdを生じ、光ディスク7のリードインエリアに記録する。

【0051】一方、ステップS1で、光ディスク7にEDiscIDと暗号化ディスクキーEKdが書き込まれていると判定された場合、ステップS8に進み、DiscID暗号化復号回路21は、この光ディスク7から読み出されたEDiscIDを、M系列符号発生回路22から供給されたM系列符号で復号して、DiscIDを得る。

【0052】ステップS9において、Kem発生モジュール23のhash関数回路25は、Kem発生モジュール23のKmメモリ24から、最新世代のマスタキーKmを読み出す。Kem発生モジュール23のhash関数回路25は、ステップS10で、上述した式(1)に従い、光ディスク7のDiscIDとマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路26に供給する。

【0053】次に、ステップS11において、Kd暗号化復号回路26は、光ディスク7から読み出された暗号化ディスクキーEKdを、hash関数回路25から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを得る。Kd暗号化復号回路26は、ディスクキーKdを、Ks暗号化回路27に出力する。

【0054】ステップS7またはS11の処理の後、乱数発生回路10は、ステップS12において、40ビットの乱数を生じ、セクタキーKsとして、Ks暗号化回路27、およびコンテンツデータ暗号化回路28に出力する。Ks暗号化回路27は、ステップS13において、Kd暗号化復号回路26（暗号化ディスクキーEKdが光ディスク7に記録されている場合）、または乱数発生回路10（暗号化ディスクキーEKdが光ディスク7に記録されていない場合）から受け取ったディスクキーKdで、乱数発生回路10から受け取ったセクタキーKsを暗号化して、暗号化セクタキーEKsを生じ、Ks暗号化回路27はまた、その暗号化セクタキーEKsを、光ディスク7のデータエリアのヘッダに記録する。

【0055】次に、ステップS14において、コンテンツデータ暗号化回路28は、セクタキーKsにより、コンテンツデータを暗号化し、光ディスク7のデータエリアのメインデータ部に記録する。

【0056】ステップS15において、暗号化部4の各回路は、全てのコンテンツデータを記録したか否かの判定を行う。全てのコンテンツデータがまだ記録されていないと判定された場合、ステップS16に進み、暗号化

部4の各回路は、光ディスク7の、まだデータを記録していないセクタにアクセスし、ステップS12を繰り返す。以下同様の処理を繰り返す。一方、ステップS15で、全てのコンテンツデータが記録されたと判定された場合、暗号化部4の各回路は、全ての記録処理を終了する。

【0057】以上のようにして、著作権者から適正なライセンスを受けるときに、与えられた所定のM系列符で、暗号化されたDiscIDを復号し、DiscIDを得ることににより、暗号化した情報が記録媒体に記録される。これにより、例えば、著作権者から適正にライセンスを受けていない者が、このディスクのコンテンツデータを既存の記録媒体（DiscIDが記録されていない記録媒体）に複製したとしても、そのコンテンツデータを、意味のある情報として再生することができない。

【0058】次に、図7のフローチャートを参照して、復号部5により行われる、コンテンツデータの再生処理を説明する。ステップS21において、EDiscID復号回路41は、光ディスク7のリードインエリアから読み出された、暗号化されたDiscIDであるEDiscIDを受け取る。また、世代判別回路49は、光ディスク7のデータエリアのヘッダを受け取る。

【0059】EDiscID復号回路41は、ステップS22において、M系列符号発生回路42から供給されたM系列符号に基づいて、EDiscIDを復号してDiscIDを得た後、Kem発生モジュール43のhash関数回路45に出力する。

【0060】次に、ステップS23において、Kem発生モジュール43のhash関数回路45は、EDiscID復号回路41から出力されたDiscIDを受け取るとともに、世代判別回路49が判別した世代に従って、Kmメモリ44から読み出されたマスタキーKmを受け取り、上述した式(1)に従い、光ディスク7のDiscIDとマスタキーKmの結合にhash関数を適用してイフェクティブマスタキーKemを算出し、EKd復号回路46に供給する。

【0061】ステップS24において、EKd復号回路46は、光ディスク7のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。EKd復号回路46は、ステップS25で、この読み出された暗号化ディスクキーEKdを、hash関数回路45から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを算出し、EKs復号回路47に出力する。

【0062】次に、ステップS26において、EKs復号回路47は、光ディスク7のデータエリアから読み出された各セクタの暗号化セクタキーEKsi（i=1,2,...）を受け取る。EKs復号回路47は、ステップS27で、この読み出された暗号化セクタキーEKsiを、EKd復号回路46から受け取ったディスクキーKdで復号して、セクタキーKsiを算出し、コンテンツデータ復号回路48に出力する。



【0063】ステップS28において、コンテンツデータ復号回路48は、光ディスク7から読み出された暗号化されているコンテンツデータを受け取る。コンテンツデータ復号回路48は、ステップS29で、この読み出された暗号化されているコンテンツデータを、Eks復号回路47から受け取ったセクタキー-Ksで復号し、再生信号として出力する。

【0064】次に、ステップS30において、復号部5の各回路は、光ディスク7のデータエリアから、全てのコンテンツデータを読み出したか否かの判定を行う。全てのコンテンツデータがまだ読み出されていないと判定された場合、ステップS31に進み、復号部5の各回路は、光ディスク7の、まだ読み出されていない次のセクタのデータの供給を受け、ステップS26以降の処理を繰り返す。全てのコンテンツデータが読み出されたと判定された場合、復号部5の各回路は、全ての再生処理を終了する。

【0065】このように、記録媒体のIDを生成し、所定のM系列符号で暗号化して、記録媒体に記録すること、著作権者から適正にライセンスを受けた者だけが、その記録媒体にアクセスできる。また、複数のマスターキー-Kmを記憶することにより、古い世代のマスターキー-Kmで暗号化されたデータでも復号（再生）することができる。

【0066】なお、上述した実施の形態においては、Kmメモリ24、44が、世代毎のマスターキー-Kmを記憶するようにしたが、最新世代のマスターキー-Kmから過去の世代のマスターキー-Kmを生成するようにしても良い。すなわち、各デバイスに1方向性関数fを記憶させ、その1方向性関数fに最新世代のマスターキー-Kmを代入することにより、その1世代前のマスターキー-Kmを作成する。さらに古いマスターキー-Kmが必要な場合には、順次1方向性関数fに繰り返しマスターキー-Kmを代入することにより、1世代つづ前の世代のマスターキー-Kmを作成する。

【0067】この1方向性関数fとしては、例えば、Hash関数やMD5（Message Diger 5）を用いることが可能である。

【0068】本発明は、光ディスク以外の記録媒体にデータを記録または再生する場合にも適用が可能である。

【0069】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【0070】この記録媒体は、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フロッピーディスクを含む）、光ディスク（CD-ROM（Compact Disk-Read Only Memory）、DVD（Digital Versatile Disk）を含む、光磁気ディスク（MD（Mini-Disk）を含む）、若しくは半導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記録されているROMや、ハードディスクなどで構成される。

【0071】

【発明の効果】本発明に記載の情報記録装置および方法、情報再生装置および方法、並びに記録媒体のプログラム、並びに記録媒体によれば、所定の世代の秘密キーを記憶し、記録媒体に記録されているデータを暗号化した秘密キーの世代に対応する秘密キーを生成し、その生成された秘密キーを用いて、記録媒体に暗号化されて記録されているデータを復号するようにしたので、記録されている秘密キーを更新した場合でも、古い秘密キーで暗号化されたデータを復号することが可能となる。

【図面の簡単な説明】

【図1】本発明を適用した光ディスク記録再生装置の一実施の形態の構成を示すブロック図である。

【図2】光ディスクに記録されるデータを説明する図である。

【図3】図1の暗号化部4の内部の構成を示す図である。

【図4】図1の復号部5の内部の構成を示す図である。

【図5】Kmメモリに記憶されるデータを説明する図である。

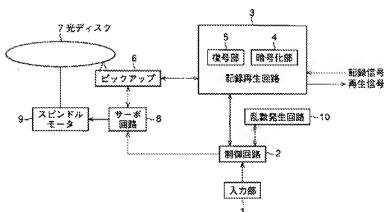
【図6】図1の暗号化部4の動作を説明するフローチャートである。

【図7】図1の復号部5の動作を説明するフローチャートである。

【符号の説明】

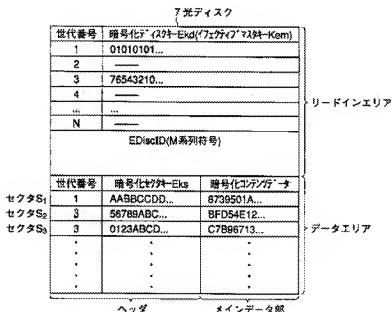
1 入力部、2 制御回路、3 記録再生回路、4 暗号化部、5 復号部、6 ピックアップ、7 光ディスク、8 サーボ回路、9 スピンドルモータ、10 乱数発生回路、21 DiscID暗号化復号回路、22 M系列符号発生回路、23 Km発生モジュール、24 Kmメモリ、25 hash関数回路、26 Kd暗号化復号回路、27 Ks暗号化回路、28 コンテンツデータ暗号化回路、41 EDiscID復号回路、42 M系列符号発生回路、43 Km発生モジュール、44 Kmメモリ、45 hash関数回路、46 EKd復号回路、47 EKS復号回路、48 コンテンツデータ復号回路、49 世代判別回路

【図1】



光ディスク記録再生装置

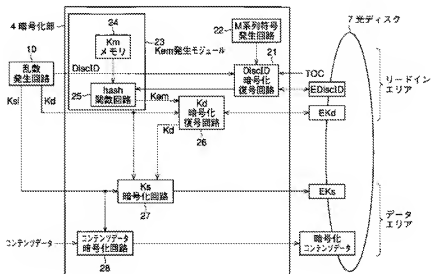
【図2】



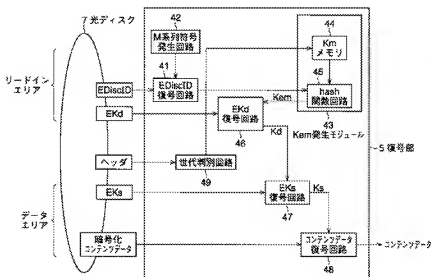
【図5】

世代番号	マスタキ-Km
1	01234567...
2	FEDCBA98...
3	00112233...
4	...
...	...
N	...

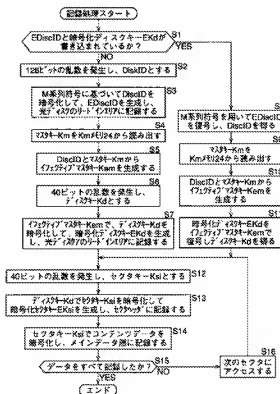
【図3】



【図4】



【図6】



【図7】

